



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/805,181

03/19/2004

Mark Delany

08226/100S142-US3

7413

38880

7590

10/10/2006

DARBY & DARBY P.C.

P.O. BOX 5257

NEW YORK, NY 10150-6257

EXAMINER

BAUM, RONALD

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 10/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/805,181	Applicant(s) DELANY, MARK	
	Examiner. Ronald Baum	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-5, 11-14 and 16-28 is/are rejected.
- 7) ☒ Claim(s) 6-10 and 15 is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 19 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date ____. | 6) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

1. Claims 1-28 are pending for examination.
2. Claims 1-5, 11-14, 16-28 are rejected.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 1, 11, 12, 16, 17, 20, 23, 26, 28 are rejected under 35 U.S.C. 101 because the disclosed invention is inoperative and therefore lacks utility. The claim phrase "if a ..." whereas there does not exist a subsequent alternative (i.e., "else ...") effectively renders the "if a ..." phrase inoperative and thus lacks utility (and is irrelevant).
4. Claims 26, 27 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The phrase "A carrier wave signal" is non-statutory. The examiner assumes for the sake of applying art that the claim is an embodied software method claim. Correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Art Unit: 2136

5. Claims 1-5, 13, 14, 18-28 are rejected under 35 U.S.C. 102(b) as being anticipated by Gupta et al, U.S. Patent 6,389,532 B1.

6. As per claim 1; "A method for message authentication, comprising:

generating a key pair associated with a domain,

wherein a public component of the key pair is

accessible to a domain name system (DNS) server that is

associated with the domain *[Abstract, figures 4-8 and*

accompanying descriptions, whereas the key pair generated is clearly

'associated' with the domain per se, and the DNS uses the public key to

verify the signature, clearly encompassing the claimed limitations as

broadly interpreted by the examiner.];

if a message originates from a sender's address associated with the domain,

employing a private component of the key pair to

digitally sign the message and

forwarding the digitally signed message towards

a recipient of the message *[Abstract, figures 4-8 and accompanying*

descriptions, whereas the key pair generated is used to verify for the purpose of

filtering messages (i.e., such that a message is forwarded or not as a function of

the filtering results) , clearly encompassing the claimed limitations as broadly

interpreted by the examiner.]; and

Art Unit: 2136

if the public component stored with the DNS server verifies that the digitally signed message originated from the domain associated with the sender's address,

employing at least one policy to

handle the verified digitally signed message for

the recipient *[Abstract, figures 4-8 and accompanying descriptions, whereas again, the purpose of filtering messages is to enable forwarding or not as a function of the filtering results. Further, the filtering criteria per se is clearly a security policy insofar as all routing of packets/session results, etc., is controlled via the said filtering criteria which is the policy, clearly encompassing the claimed limitations as broadly interpreted by the examiner.]”*.

As per claim 20, this claim is the server embodied apparatus claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; “A server for message authentication, comprising:

a memory for storing instructions;

a processor for enabling actions based on the stored instructions, including:

generating a key pair associated with a domain,

wherein a public component of the key pair is

accessible to a domain name system (DNS) server that is

associated with the domain;

if a message originates from a sender's address associated with the domain,

employing a private component of the key pair to
digitally sign the message and
forwarding the digitally signed message towards
a recipient of the message; and
if the public component stored with the DNS server verifies that the digitally
signed message originated from the domain associated with the sender's address,
employing at least one policy to
handle the verified digitally signed message for
the recipient.”.

As per claim 23, this claim is the client embodied apparatus claim for the method claim 1
above, and is rejected for the same reasons provided for the claim 1 rejection; “A client for
message authentication, comprising:

a memory for storing instructions;

a processor for enabling actions based on the stored instructions, including:

generating a key pair associated with a domain,

wherein a public component of the key pair is

accessible to a domain name system (DNS) server that is

associated with the domain;

if a message originates from a sender's address associated with the domain,

employing a private component of the key pair to

digitally sign the message and

forwarding the digitally signed message towards
a recipient of the message; and
if the public component stored with the DNS server verifies that the digitally
signed message originated from the domain associated with the sender's address,
employing at least one policy to
handle the verified digitally signed message for
the recipient.”.

As per claim 26, this claim is the embodied software claim for the method claim 1 above,
and is rejected for the same reasons provided for the claim 1 rejection; “A carrier wave signal
that includes instructions for performing actions, comprising:

generating a key pair associated with a domain,
wherein a public component of the key pair is
accessible to a domain name system (DNS) server that is
associated with the domain;
if a message originates from a sender's address associated with the domain,
employing a private component of the key pair to
digitally sign the message and
forwarding the digitally signed message towards
a recipient of the message; and
if the public component stored with the DNS server verifies that the digitally signed
message originated from the domain associated with the sender's address,

employing at least one policy to
handle the verified digitally signed message for
the recipient.”.

As per claim 28, this claim is the means plus function claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; “An apparatus for message authentication, comprising:

a means for generating a key pair associated with a domain,
wherein a public component of the key pair is
accessible to a domain name system (DNS) server that is
associated with the domain;

a means for

employing a private component of the key pair to
digitally sign the message and
forwarding the digitally signed message towards
a recipient of the message

if a message originates from a sender's address associated with the domain; and

a means for

employing at least one policy to
handle the verified digitally signed message for
the recipient

if the public component stored with the DNS server verifies that the digitally signed message originated from the domain associated with the sender's address.”.

7. Claim 2 *additionally recites* the limitation that; “The method of claim 1, wherein employing at least one policy, further comprises
- employing an unverified policy to
- handle each message
- for the recipient that originates
- from a sender's domain
- that is unverifiable,
- wherein the unverified policy
- enables at least one action including
- partial rejection, and
- complete rejection.”.

The teachings of Gupta et al suggest such limitations (Abstract, figures 4-8 and accompanying descriptions, whereas again, the purpose of filtering messages is to enable forwarding or not as a function of the filtering results. Further, the filtering criteria per se is clearly a security policy insofar as all routing of packets/session results, etc., is controlled via the said filtering criteria which is the policy, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

8. Claim 3 *additionally recites* the limitation that; “The method of claim 1, wherein

employing at least one policy, further comprises
employing a verified policy to
handle each verified digitally signed message
for the recipient that originates from
the verified domain of the sender,
wherein the verified policy
enables at least one action including
complete acceptance,
complete rejection,
preferential acceptance,
partial rejection, and
partial acceptance.”.

The teachings of Gupta et al suggest such limitations (Abstract, figures 4-8 and accompanying descriptions, whereas again, the purpose of filtering messages is to enable forwarding or not as a function of the filtering results. Further, the filtering criteria per se is clearly a security policy insofar as all routing of packets/session results, etc., is controlled via the said filtering criteria which is the policy, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

9. Claim 4 *additionally recites* the limitation that; “The method of claim 1, wherein
employing at least one policy, further comprises
employing a system policy to

handle each verified digitally signed message
for each recipient
in a message system,
wherein the system policy
enables at least one action
for each recipient in the message system including
complete acceptance,
complete rejection,
preferential acceptance,
partial acceptance, and
partial rejection.”

The teachings of Gupta et al suggest such limitations (Abstract, figures 4-8 and accompanying descriptions, whereas again, the purpose of filtering messages is to enable forwarding or not as a function of the filtering results. Further, the filtering criteria per se is clearly a security policy insofar as all routing of packets/session results, etc., is controlled via the said filtering criteria which is the policy, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

10. Claim 5 *additionally recites* the limitation that; “The method of claim 1, wherein employing at least one policy, further comprises
employing a user policy for a particular recipient to
handle the verified digitally signed message,

Art Unit: 2136

wherein the user policy
enables at least one action
for the particular recipient including
complete acceptance,
complete rejection,
preferential acceptance,
partial acceptance, and
partial rejection.”.

The teachings of Gupta et al suggest such limitations (Abstract, figures 4-8 and accompanying descriptions, whereas again, the purpose of filtering messages is to enable forwarding or not as a function of the filtering results. Further, the filtering criteria per se is clearly a security policy insofar as all routing of packets/session results, etc., is controlled via the said filtering criteria which is the policy, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

11. Claim 13 *additionally recites* the limitation that; “The method of claim 1, further comprising

displaying a positive visual indication of

at least one action, including
complete acceptance,
preferential acceptance, and
partial acceptance

of the verified digitally signed message,
wherein the positive indication includes at least one of
text,
graphic,
picture, and
color.”.

The teachings of Gupta et al suggest such limitations (Abstract, figures 4-8 and accompanying descriptions, whereas again, the purpose of filtering messages is to enable forwarding or not as a function of the filtering results. Further, the routing of packets/session results, etc., through associated routing network appliances is such that said appliances have multicolored LED indicators that annunciate the state/status of traffic (acceptance status/state allowed, blocked, partially blocked, faulty, etc.), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

12. Claim 14 *additionally recites* the limitation that; “The method of claim 1, further comprising

displaying a negative visual indication of
at least one action, including
complete rejection, and
partial rejection
of the verified digitally signed message
wherein the negative indication includes at least one of

Art Unit: 2136

text,
graphic,
picture, and
color.”.

The teachings of Gupta et al suggest such limitations (Abstract, figures 4-8 and accompanying descriptions, whereas again, the purpose of filtering messages is to enable forwarding or not as a function of the filtering results. Further, the routing of packets/session results, etc., through associated routing network appliances is such that said appliances have multicolored LED indicators that annunciate the state/status of traffic (acceptance status/state allowed, blocked, partially blocked, faulty, etc.), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

13. Claim 18 *additionally recites* the limitation that, “The method of claim 1, further comprising

generating a personal digital certificate for the sender

based on

the public component and

the private component

of the key pair

associated with the domain;

providing

a public component of the personal digital certificate to

the recipient along with
the verified digitally signed message; and
enabling the recipient to
subsequently provide
a response message to the sender that is
automatically encrypted with
the public component of
the sender's personal digital certificate.”.

The teachings of Gupta et al suggest such limitations (Abstract, figures 4-8 and accompanying descriptions, whereas the public key pair (source or sender side) generated and associated with a certification server, are used for message authentication of the verified digitally signed message, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

14. Claim 19 *additionally recites* the limitation that; “The method of claim 18, wherein the personal digital certificate is associated with
an address of the sender.”.

The teachings of Gupta et al suggest such limitations (Abstract, figures 4-8 and accompanying descriptions, whereas the public key pair (source or sender side) generated and associated with a certification server, are used for message authentication of the verified digitally signed message, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

15. Claim 21 *additionally recites* the limitation that; “The server of claim 20, wherein

the at least one policy includes at least one of

an unverified domain policy,

a verified domain policy,

a new domain policy,

a system policy,

a user policy,

a statistics policy, and

a third party policy.”.

The teachings of Gupta et al suggest such limitations (Abstract, figures 4-8 and accompanying descriptions, whereas again, the purpose of filtering messages is to enable forwarding or not as a function of the filtering results. Further, the filtering criteria per se is clearly a security policy insofar as all routing of packets/session results, etc., inclusive of filtering parameters dealing with domain (verified, unverified, new, etc.), user, system, third party, etc., is controlled via the said filtering criteria which is the policy, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

16. As per claim 22, this claim is the combined method claims 18, 19 above, and is rejected for the same reasons provided for the claim 18, 19 rejections; “The server of claim 20, the actions further comprising:

generating a personal digital certificate for the sender

based on

the public component and

the private component
of the key pair
associated with the domain,
wherein the personal digital certificate is associated with
an address of the sender;
providing
a public component of the personal digital certificate to
the recipient along with
the verified digitally signed message; and
enabling the recipient to
subsequently provide
a response message to the sender that is
automatically encrypted with
the public component of
the sender's personal digital certificate.”

17. Claim 24 *additionally recites* the limitation that; “The client of claim 23, wherein
the at least one policy includes at least one of
an unverified domain policy,
a verified domain policy,
a new domain policy,
a system policy,

Art Unit: 2136

a user policy,
a statistics policy, and
a third party policy.”.

The teachings of Gupta et al suggest such limitations (Abstract, figures 4-8 and accompanying descriptions, whereas again, the purpose of filtering messages is to enable forwarding or not as a function of the filtering results. Further, the filtering criteria per se is clearly a security policy insofar as all routing of packets/session results, etc., inclusive of filtering parameters dealing with domain (verified, unverified, new, etc.), user, system, third party, etc., is controlled via the said filtering criteria which is the policy, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

18. As per claim 25, this claim is the combined method claims 18, 19 above, and is rejected for the same reasons provided for the claim 18, 19 rejections; “The client of claim 23, the actions further comprising:

generating a personal digital certificate for the sender

based on

the public component and

the private component

of the key pair

associated with the domain,

wherein the personal digital certificate is associated with

an address of the sender;

providing
a public component of the personal digital certificate to
the recipient along with
the verified digitally signed message; and
enabling the recipient to
subsequently provide
a response message to the sender that is
automatically encrypted with
the public component of
the sender's personal digital certificate.”.

19. As per claim 27, this claim is the combined method claims 18, 19 above, and is rejected for the same reasons provided for the claim 18, 19 rejections; “The carrier wave signal of claim 26, the actions further comprising:

generating a personal digital certificate for the sender
based on
the public component and
the private component
of the key pair
associated with the domain,
wherein the personal digital certificate is associated with
an address of the sender;

providing
a public component of the personal digital certificate to
the recipient along with
the verified digitally signed message; and
enabling the recipient to
subsequently provide
a response message to the sender that is
automatically encrypted with
the public component of
the sender's personal digital certificate.”.

Allowable Subject Matter

20. Claims 6-12, 15-17 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

21. Claim 6 ***additionally recites*** the limitation that; “The method of claim 1, wherein employing at least one policy, further comprises
employing a third party to
provide a score for a particular domain to
a message system for
determining a score policy on

handling each verified digitally signed message
that originates from the scored domain,
wherein the score policy
enables at least one action including
complete acceptance,
complete rejection,
preferential acceptance,
partial acceptance, and
partial rejection.”.

22. Claim 7 *additionally recites* the limitation that; “The method of claim 6, wherein
the third party aggregates
information from at least one recipient
in a plurality of message systems for
determining the score for the domain.”.

23. Claim 8 *additionally recites* the limitation that; “The method of claim 6, further
comprising
enabling the third party to
provide a suggested score policy for
handling each verified digitally signed message
from the scored domain based at least in part on

the aggregated information,
wherein the suggested scored policy
enables at least one action including
complete acceptance,
complete rejection,
preferential acceptance,
partial acceptance, and
partial rejection.”.

24. Claim 9 *additionally recites* the limitation that, “The method of claim 1, wherein
employing at least one policy, further comprises

employing a statistics policy based on at least one statistic regarding a plurality of
verified digitally signed messages that have previously originated from the verified
domain,

wherein the statistics policy
enables the handling of each message that originates
from the previously verified domain, and

wherein the statistics policy
enables at least one action including
complete acceptance,
complete rejection,
preferential acceptance,

partial acceptance, and
partial rejection.”.

25. Claim 10 *additionally recites* the limitation that; “The method of claim 9, further comprising

determining a trend for messaging behavior

in regard to a plurality of messages originating

from the domain over a period of time.”.

26. Claim 11 *additionally recites* the limitation that; “The method of claim 10, if the trend is determined to represent negative messaging behavior for the domain,

employing at least a length of the trend to

enable a change in at least one policy associated with

the handling of verified digitally signed message for

the recipient.”.

27. Claim 12 *additionally recites* the limitation that; “The method of claim 10, if the trend is determined to represent positive messaging behavior for the domain,

employing at least a length of the trend to

enable a change in at least one policy associated with

the handling of verified digitally signed message for

the recipient.”.

Art Unit: 2136

28. Claim 15 *additionally recites* the limitation that, “The method of claim 1, further comprising

automatically segmenting an inbox to

at least temporarily store

each verified digitally signed message in accordance with

the at least one policy that enables at least one action, including

complete rejection,

complete acceptance,

preferred acceptance,

partial rejection, and

partial acceptance.”.

29. Claim 16 *additionally recites* the limitation that, “The method of claim 1, wherein employing at least one policy, further comprises

if it is determined that the domain is relatively new to a messaging system,

employing a new domain policy for

handling an amount of verified digitally signed messages that are

less than a predetermined limit

over a period of time,

wherein each message

less than the predetermined limit

is handled with at least

partial acceptance.”.

30. Claim 17 *additionally recites* the limitation that; “The method of claim 1, wherein employing the policy, further comprises

if it is determined that the domain is relatively new to a messaging system,

employing a new domain policy for

handling an amount of verified digitally signed messages that are

less than a predetermined limit

over a period of time,

wherein each message

that is greater than the predetermined limit

is handled with at most

partial rejection.”.

Art Unit: 2136

Conclusion

31. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Nasser Moazzami
10/04/06

Ronald Baum